While cyber threats may not be in your control, your cybersecurity strategy is and you should be looking at a risk-based approach. This cyber security training course prepares managers and senior executives to understand, assess, and take a proactive approach in cybersecurity. With this course, you gain the knowledge of the threats faced by organizations and where they come from, what is required to create a Cyber Security Compliance Program, what is a Cyber Risk Assessment and why it is needed, how to rate your level of risk and how to perform a Cyber Risk Assessment. You will also cover what is a Cybersecurity Framework and what is required to prepare an Incident Response Plan.

Who Should Attend

Candidates should have a general awareness of information security and the need to respond to such events.

- ❖ Executives
- ❖ managers
- ❖ Security officers
- ❖ Data Protection Officers (DPO)

Outcome

This course will provide you with the training and knowledge to make informed decisions to put your organization's security strategy in place and understand the importance of cyber security compliance.

Course Content

- ❖ Introduction
- ❖ Why is it Necessary to Protect Against Cyber Security Threats?
- ❖ Data Breach Trends
- ❖ Overview of Cyber Legislation
- ❖ Where do Cyber Threats Come from?

- ❖ Examples of Cyber Threats
- ❖ What is Cyber Security Compliance?
- ❖ 5 Steps to Creating a Cyber Security Compliance Program
- ❖ What is a Cyber Risk Assessment?
- ❖ Why Perform a Cyber Risk Assessment?

- ❖ What is Risk?
- ❖ Risk Assessment Model
- ❖ How to Perform a Cyber Risk Assessment?
- ❖ Cybersecurity Frameworks
  - o NIST Cybersecurity Framework
  - o Cyber Assessment Framework
- ❖ Preparing an Incident Response Plan

Further Information - **For further information, please contact E5h Forensic Solutions. Email: training@e5hforensics.com**